

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (currently amended) A method of providing access control for user terminals connected to a private network, wherein said terminals access a computer network enabling exchange of information via a private access node to which said terminals are connected and an access server, the method comprising:

temporarily storing a multimedia data stream received from said computer network and addressed to a user terminal of said user terminals connected to said private network in response to an access request from said user terminal in order to perform filtering based on data content of said multimedia data stream, said filtering, authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria provided from said private network and applied to the multimedia data stream received at said private access node, and

analyzing a signature included in said multimedia data stream for the purpose of said filtering.

2. (Previously Presented) The method claimed in claim 1, wherein said multimedia data stream received from said computer network is stored temporarily before it is transmitted to said user terminal depending on results of said filtering.

3. (Cancelled)

4. (Previously Presented) The method claimed in claim 1, wherein transfer of said multimedia data stream received from said computer network to a user terminal is temporarily delayed pending determination of conformance of said multimedia data stream which has been received with particular standards and then transmitted to said terminal if conformance is found.

5. (previously presented) The method claimed in claim 4, wherein temporarily delayed data, which comprises said multimedia data stream stored in the determination of conformance, is retained to enable a further check in the event of non-conformance, either in respect of data received on detection of non-conformance, in which case the multimedia data stream is interrupted, or in respect of all data of the multimedia data stream received, without said multimedia data stream being interrupted.

6. (Previously Presented) The method claimed in claim 4, wherein data for which non-conformance has been detected in said multimedia data stream is retained to enable interruption of a subsequently received multimedia data stream before complete analysis of said subsequently received multimedia data stream if said data is detected again in said subsequently received multimedia data stream.

7. (Previously Presented) The method claimed in claim 1, further comprising counting, for control purposes, the number of times that data of a particular content is received, if said content is found in said multimedia data stream which is temporarily stored, after it has been received from said computer network in at least one data stream addressed to a particular terminal.

8. (Previously Presented) The method claimed in claim 2, further comprising performing signature analysis for at least temporarily blocking transmission of said multimedia data stream received from said network to a user terminal if said multimedia data stream incorporates a signature characteristic of restricted signaling rights.

9. (Previously Presented) The method claimed in claim 2, further comprising performing an identifier search analysis on said multimedia data stream addressed to a user

terminal to authorize transmission of said multimedia data stream to said terminal if an identifier is found in the multimedia data stream addressed to said terminal.

10. (previously presented) An apparatus for providing access control for user terminals connected to a private network, wherein said terminals access a computer network enabling exchange of information via a private access node to which said terminals are connected and a service provider, organized to authorize or block transmission of said data stream to said terminals, the apparatus comprising:

a storage unit for temporarily storing a multimedia data stream received from said computer network and addressed to a user terminal of said user terminals connected to said private network in response to an access request from said user terminal,

a control logic unit for filtering said multimedia data stream stored in said storage unit, said filtering authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria provided from said private network and applied to data content which comprises said multimedia data stream received at said private access node, and analyzing a signature included in said multimedia data stream for the purpose of said filtering.

11. (new): The method of providing access control for user terminals connected to a private network according to claim 1, wherein performing filtering based on data content of said multimedia data stream comprises analyzing an information of said multimedia data.

12. (new): The method of providing access control for user terminals connected to a private network according to claim 1, wherein temporarily storing the multimedia data stream comprises storing only a part of the multimedia data stream.

13. (new): The method of providing access control for user terminals connected to a private network according to claim 1, wherein the signature indicates an existence of restrictions on a use of the multimedia data stream.